Ficha técnica

Simplifique el cumplimiento de la Directiva NIS2 sobre la seguridad de las identidades con una gestión del acceso privilegiado de última generación

¿Está preparada su organización para la Directiva NIS2?

La Directiva NIS2 [Directiva (UE) 2022/2555] entrará en vigor en octubre de 2024. La Directiva NIS2 amplía el alcance de su predecesora, la Directiva NIS sobre redes y sistemas de información. La nueva versión abarca más sectores y tipos de organizaciones, debido a la cada vez mayor dependencia de las tecnologías digitales y el aumento en el volumen de amenazas cibernéticas. La directiva tiene como objetivo mejorar la seguridad de las redes y los sistemas de información dentro de la UE, garantizando un nivel elevado común de seguridad cibernética. Con la revisión de la directiva, los estados miembros de la UE tienen como objetivo defender mejor a los sectores críticos del sector frente a los ataques de ransomware, las vulnerabilidades de la cadena de suministro y mucho más.

La Directiva NIS2 incluye más sectores industriales que la original. Además, los requisitos no solo se aplican a las organizaciones y sus empleados directos, sino también a los subcontratistas y los proveedores de servicios con los que trabajan.

Sectores de la Directiva NIS	Sectores adicionales de la Directiva NIS2	
• **Banca** • **Infraestructura digital** • **Proveedores de servicios digitales** • **Mercado financiero Infraestructura** • **Energía** • **Atención sanitaria** • **Transporte** • **Suministro de agua**	• Productos químicos • Proveedores digitales (plataformas en línea de compraventa, motores de búsqueda y redes sociales) • Productores, procesadores y distribuidores de alimentos • Atención sanitaria (dispositivos médicos esenciales, productos farmacéuticos, investigación y desarrollo) • Servicios postales y de mensajería	• Administración pública • Espacio • Aguas residuales • Fabricación de productos esenciales (ordenadores, dispositivos electrónicos, dispositivos médicos, vehículos motorizados) • Proveedores de redes o servicios públicos de comunicaciones electrónicas

Coste y peligros del incumplimiento de la Directiva

Si una organización no cumple con lo establecido en la Directiva NIS2, puede enfrentarse a varias consecuencias diseñadas para garantizar que las distintas entidades se tomen en serio sus obligaciones en materia de seguridad cibernética. La naturaleza y la gravedad de estas consecuencias pueden variar en función de la legislación específica de cada Estado miembro de la UE, ya que son ellos los responsables de transponer las directivas de la UE a su legislación nacional. Sin embargo, la Directiva NIS2 brinda un marco para estas sanciones con el objetivo de conseguir armonizar el enfoque en toda la UE. Entre las posibles consecuencias cabe citar las siguientes:

- Sanciones económicas
- Multas periódicas
- Obligación de tomar medidas específicas
- Anuncios públicos y daños a la reputación
- Restricciones operativas
- Responsabilidad por daños y perjuicios

La ejecución de estas consecuencias la llevan a cabo las autoridades nacionales designadas por cada Estado miembro de la UE.

Olvídese de quebraderos de cabeza en torno a la conformidad con la Directiva NIS2 gracias a KeeperPAM

Las organizaciones de la Unión Europea pueden hacer uso de la solución de gestión del acceso privilegiado (PAM) de última generación de Keeper para cumplir de forma fácil y rentable la Directiva NIS2. Como ofrece controles de acceso granulares basados en roles (RBAC), Keeper permite a los administradores de TI gestionar el acceso a las cuentas privilegiadas en toda la organización, lo que garantiza que los usuarios solo tengan los permisos necesarios para desempeñar sus funciones particulares.Las prestaciones avanzadas de generación de informes brindan información clara sobre las actividades de las cuentas privilegiadas, lo que ayuda a que la supervisión sea continua y simplifica las auditorías necesarias para el cumplimiento de la Directiva NIS2. Keeper también faculta a las organizaciones de todos los tamaños para aplicar las prácticas recomendadas en materia de seguridad cibernética, como el uso de contraseñas seguras y exclusivas o la habilitación de la autenticación multifactor (MFA). La piedra angular de la solución de Keeper es su modelo de cifrado conocimiento cero, que garantiza que los datos sensibles estén protegidos por la seguridad líder del sector, lo que la convierte en la opción ideal para las organizaciones de la UE que desean cumplir con los estándares de la NIS2 y mejorar su situación general respecto de la seguridad cibernética.

Optimice el cumplimiento de la Directiva NIS2

Requisito	Solución
Párrafo 49: Políticas de higiene cibernética	**Establezca políticas seguras de higiene cibernética con la gestión de contraseñas y el acceso de privilegios mínimos.** El gestor de contraseñas para empresas líder del sector de Keeper crea, guarda y gestiona contraseñas complejas y exclusivas para todos los usuarios. Los controles de acceso basados en roles (RBAC) permiten a los administradores gestionar de forma precisa los permisos de los usuarios, lo que garantiza que las personas solo tengan acceso a los recursos necesarios para sus funciones laborales y el privilegio mínimo en toda la organización.
Párrafo 54: Ransomware	**Proteja los datos y los sistemas del ransomware.** Keeper aplica el uso de contraseñas seguras y exclusivas y la autenticación MFA para todos los usuarios y dispositivos de una organización. KeeperPAM centraliza los secretos en una bóveda segura y puede configurarse para rotar las credenciales automáticamente. Keeper también proporciona acceso seguro a bases de datos e infraestructuras remotas sin exponer credenciales. Los informes detallados, las alertas en tiempo real y el monitoreo de la dark web permiten a las organizaciones detectar rápidamente las credenciales no seguras o vulneradas para mitigar posibles amenazas.
Párrafo 62: Información oportuna sobre las vulnerabilidades	**Acceda a información correcta y oportuna sobre las vulnerabilidades e implemente un procedimiento adecuado para tomar medidas de mitigación.** El completo panel sobre riesgos de Keeper proporciona a los administradores una visión general instantánea de la actividad de los usuarios y el estado general de la seguridad, incluidas las contraseñas o credenciales no seguras o reutilizadas que se hayan encontrado en la dark web.
Párrafo 85: Seguridad de la cadena de suministro	**Gestione la seguridad de la cadena de suministro y las relaciones con los proveedores.** Keeper Secrets Manager proporciona una solución totalmente gestionada basada en la nube para acceder a secretos, almacenarlos y rotarlos. Elimina la distribución no controlada de información confidencial dentro del entorno. Esto incluye contraseñas, claves de API, claves de contraseñas de bases de datos, certificados y otros datos sensibles.
Párrafo 89: Prácticas de higiene cibernética para los usuarios	**Establish strong cyber hygiene practices, from zero-trust principles to identity and access management.** Establezca prácticas seguras de higiene cibernética, desde los principios de confianza cero hasta la gestión de identidades y accesos. Keeper gestiona los permisos de acceso y monitorea la actividad de todos los usuarios de una organización combinando los RBAC, el almacenamiento seguro de credenciales, la gestión de sesiones, la integración de la autenticación MFA y la elaboración de informes y la auditoría detallados. Keeper centraliza la gestión de las cuentas privilegiadas para un control eficiente del acceso, utiliza los RBAC para garantizar que los usuarios solo tengan acceso a lo que necesitan para sus funciones, guarda las credenciales de forma segura en bóvedas cifradas, monitorea y registra las sesiones para fines de seguridad y conformidad, mejora la seguridad con la autenticación MFA y ofrece registros de auditoría completos para todas las acciones de los usuarios privilegiados.
Párrafo 98: Cifrado de extremo a extremo para los proveedores de comunicaciones públicas	**Haga uso del cifrado de extremo a extremo para reforzar la seguridad.** Keeper es un proveedor de seguridad conocimiento cero.El conocimiento cero es una arquitectura de sistemas que garantiza los más altos niveles de seguridad y privacidad. El cifrado y el descifrado de los datos siempre se realiza de forma local en el dispositivo del usuario. Keeper es la plataforma de seguridad de contraseñas más segura, certificada, probada y auditada del mundo. Keeper tiene las certificaciones SOC2 e ISO27001 más antiguas del sector y cumple con el Marco de privacidad de datos UE-EE. UU., que representa la ampliación al Reino Unido de este mismo marco y del Marco de privacidad de datos Suiza-EE. UU., según lo establecido por el Departamento de Comercio de los Estados Unidos.
Párrafo 102: Notificación obligatoria de incidentes	**Los incidentes deben notificarse en las 24 horas posteriores a su detección.** El módulo de alertas e informes avanzados de Keeper notifica a los administradores de eventos de más de 200 tipos de eventos para que puedan generar informes personalizados con opciones integradas de envío de notificaciones a Slack, Teams, correos electrónicos u otras soluciones de mensajería mediante un webhook.